EFFECTIVE MULTICAST COMMUNICATION USING MQTT PROTOCOL AND HARDY WALL ALGORITHM IN SIOT

S.Jayasri[1] , Dr. R.Parameswari[2]
[1]Research Scholar, Department of Computer Science, School of Computing Sciences,
Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, 600 117
[2]Associate Professor, Department of Computer Science, School of Computing Sciences,
Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, 600 117

Abstract

The Social Internet of Things (SIoT) is a relatively new research field that builds on the foundation of the Internet of Things (IoT) and Social Computing (SC). Along with Wireless Sensor Network (WSNs), SIoT have been widely explored for all common functionalities related to Computer networks and Machine to Machine interfaces [1]. In recent studies, technology of SIoT is being explored in healthcare and intelligent transportation system. Due to restricted energy sources [2] in WSNs, cloud system is employed to satisfy the requirements of users in terms of storage services. Likewise, Social Internet of Things (SIoT) is employed for achieving secured authentication via clustering approaches. Routing protocols is the main key indicator in Wireless Sensor Networks (WSNs). Most of the routing protocols were designed on the basis of single hop and multiple hop clustering approaches. Social Internet of Things (This paper focuses on bringing in an effective group key generation for multicast communication in Social Internet of Things (SIoT) and also aims to discuss and analyze about the MQTT Protocol and Hardy wall algorithm.

Keywords *— Social Internet of Things (SIoT), Wireless Sensor Network (WSN), MQTT Protocol, Hardy wall Algorithm.*

1. INTRODUCTION

The Social Internet of Things is an advanced IoT paradigm in which various IoT devices communicate and form relationships with one another. The devices are the primary physical objects connected to the system. The system includes multiple sensors, actuators, data management, user interface and protocols. Energy distribution [3] is one of the key parameters that makes the sensor nodes available throughout the network communication ends. It also increases the density of the nodes. Some a huge scale sensor networks is applied with SioT, so as to identify the secured control system, even at peak time. Messaging Queuing Telemetry Transport (MQTT) is a publish/subscribe messaging protocol that runs on top of the TCP/IP protocol suite.

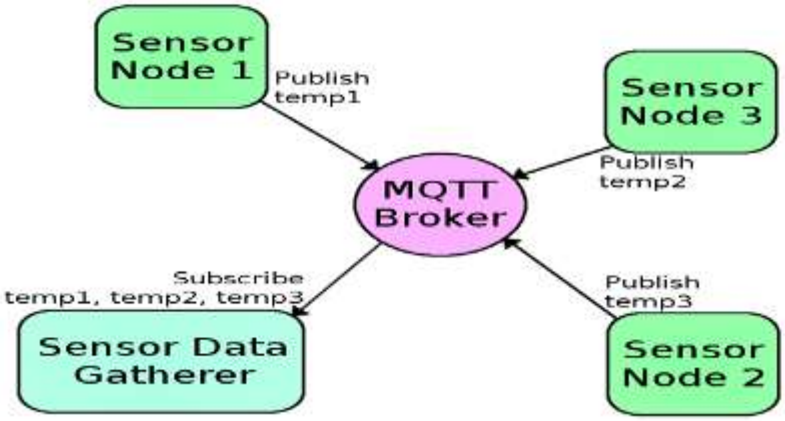

Figure 1 MQTT Protocol

Nodes are dynamically formed via clustering approaches [4], so as to reduce the time taken for data transmission. In heterogeneous environment, node density increases when energy function is activated. Lightweight hash based authentication schemes were explored to provide efficient security among users, end node and the gateway nodes, even at remote areas. Robustness of the authentication protocols were lowered due to invasion of attacks such as sybil, replay, guessing, forgery and brutal force. Likewise, data collision and congestion due to computational load are also the reasons for lowered performance of network routing protocols [5]. Therefore, the design of SioT authentication schemes should concentrate on low computational costs, power constrained and processing capability. These parameters are need to be encountered while designing cryptographic algorithms and protocols.

2. LITERATURE REVIEW

This section presents the existing security and privacy techniques in routing protocols of wireless environment. The survey covers three security aspects and they are explained as follows:

2.1 Group key establishment in IoT:

Group key establishment is defined as the process of issuing a common key among the authorized users in a group. Several security mechanisms are been established to secure the group key, yet the precise solution is not found. Generally, Group key establishment composed of two classes, group key agreement and group key transport. The shared secret is derived from the former key system, in which all entities contribute to their secret. Author in [6] presented a batch-based group key management protocol for the Internet of Things (IoT) through a key distribution centre. Under multicast group systems, this protocol performs dynamically to generate the keys and verifying among its groups, irrespective of number of sensor nodes deployed. Privacy and integrity of the sensitive data is not assured. Author in [7] presented a time-driven protocols that generated the secret keys for the active sensor nodes. It is not reliable for realistic wireless environment. Along with that, authentication of the users and its group head is not focussed which suspects to reply attacks.

Author in [8] presented a ECC-centralized group key establishment protocols that utilized certified agents. In order to generate public/ private key pairs, a certificate agents was used for verifying the wireless users among the groups. Anyhow, it is expensive in view of computational overheads. A collaborative group key system to detect the smart objects was proposed by [9]. Here, global key is generated for each collaborated members based on tree structure. Since bottom up fashion is processed for key updation process, the authors has employed symmetric encryption process for authenticating the users with base station. Concept of secret sharing schemes was introduced to reduce the computational overheads during accumulation of multiple sharing schemes. Likewise, the shared secret key shall reconstructed by only when all secret shares are combined. Conventional schemes [10] has consumed high storage cost due to the usage of polynomials and the key encoding models. Henceforth, some researchers has focussed on XoR operation to ensure high-end security with lowered computational storage, storage cost and the privacy maintenance. In [11], a distributed key management protocol for IoT systems that employed secret sharing techniques and the CA, so as to authenticate the users and privacy assurance. This system has also operated in offline environment. Since polynomial key generation was employed, the secret scheme has ensured the computational expenses without depleting more energy. It is not suitable for realistic environment due to higher time taken for signature verification process.

2.2 Authentication in IoT:

The efficiency of the security mechanisms is assessed by its authentication process. The primary goal of authentication is to prevent unauthorised users from performing actions. Generally, authentication based security mechanisms are designed on the basis of knowledge, possession and biometric aspects. Author in [12] suggested an authentication scheme for WSNs environment in hierarchical process. Since lightweight security primitives were used for computation purposes, it scalable for all network communication environments. Chance of reply attacks and DdoS attacks are highly possible in this environment. ECC-based user authentication scheme was employed to detect the security attacks as well as providing security to the systems done by [13]. System has detected the possible attacks with high false positive rates. Data availability and the data integrity in heterogeneous environment are ensured via access control scheme via

[14]. A lightweight authentication protocols was designed for IoT environment where the users can approach the sensor networks without any gateway process. It has significantly reduced the verification time, yet the response time between IoT and WSNs environment is little higher. Some security schemes are feeble in offline environment and thus more prone to password guessing and impersonation attacks. In [15], the authors reviews the merits and demerits of the existing authentication protocols. Additionally, the importance of detecting password guessing and impersonation attacks. In relation to the preceding study, the author in [16] investigated a multi-gateway model for an efficient user authentication process and key agreement schemes. System has proved its efficiency in energy consumption and scalability, yet the user-anonymity is not focussed.

2.3 SLP (Source Location Privacy):

Source location privacy refers to the ability to preserve and protect the location events reported by sensor nodes. Initially, it was studied by [17] where the authors tried to enhance the games of Panda Hunter. The main theme of this game is to preserve the location of pandas by monitoring its behavior under large sensor network applications. It is observed that the hunter takes control over the messages shared to the network and then hunting process occurred. This scenario has engaged the author to explore the significance of the source location privacy, so as to prevent the actions carried out by attackers. This, as base, different privacy challenges in IoT environment was resolved. First of all, the privacy of a user is leaked in two ways, one is leakage of the data and other is leakage of data by network/ device fault. Traffic created in packets has enabled the adversaries to take control over data by continuous monitoring of its behavior pattern. Author in [18] improved the panda hunter model for its source location issue. Here, the sensor nodes splits its nearest nodes into two crispy sets by its present position. Then, a random walk is employed over until the packet reaches the correct destination node. By doing so, source location issue was resolved for small-scale networks.

Author in [19] suggested an improved SLP process by deploying phantom routing. In general, phantom routing performs in two stages, In the first stage, random walk is used to direct packets to phantom nodes, and in the second stage, single path routing is used for packet transmission. Unicast protocols are used for total hops during the initial stage of message processing. Messages are then routed to the sink using a single path. Despite the fact that the author has ensured that energy consumption is kept to a minimum, the use of single path routing increased the performance of adversaries. And, in some cases, the communication overheads was also enhanced. Similar study was enhanced by [20] using Greedy Random Walk (GROW) approaches. At first, the sink tooks n-hop random walks which is forwarded to the source that in turn takes the m-hop random walk. Then, the intersected paths was taken as shortest route path and thus the data is being transmitted. Since it deployed local mechanisms, the intersected paths are easily threatened by network environment. In [21], privacy aware random parallel routing scheme was employed on different routing schemes. Hop by hop mechanism was taken for expanding the time for finding the detecting the location of source nodes. Since non-intersecting paths are taken, the group impersonation attack prevention is least focused.

Phantom routing with location angle was introduced by [22] that takes direct random walk approach. Here, 33 phantom sources was taken for experimental purpose. Then, the angles between those sources are estimated and also arrival time was computed. Henceforth, it reduced the hops count but the privacy of sensitive data is not assured. Additionally, energy of the node is not maintained until the entire packet traversal process. In [23], the Location privacy routing protocols was formulated that performed by categorizing the neighboring nodes into two different lists, namely closer and farthest list. Based on the list, the nodes are selected for communication purposes. It devised the communication path yet the cost factor is not analyzed. Even Though, privacy is stronger, the rate of fake packet injection is higher during direct random walk process [24]. Henceforth, the privacy challenges in SLP will be improved by deploying multipath approaches. Likewise, prevention of fake messages has taken the SLP into next level i.e large scale networks. By ensuring the privacy in heterogeneous sources and the session based routing protocols has improved the SLP for reliable packet delivery system [25].

3. PROBLEM STATEMENT

As we know, WSNs are self-organizing networks made up of various sensor nodes. Routing protocols are combined with location information to detect resource usage among destination nodes, source nodes, and the base station in order to monitor the resource utilization of sensor nodes. By applying hop-by-hop backtracking techniques, the attackers can’t easily trace the assets of source nodes. Henceforth, the privacy of the source nodes has to be addressed. Prior Source location privacy methods was employed that increased the deployment of routing paths by approaching phantom routing, multi-paths and eliminated the false messages. In some cases, the routing protocols will change its behavior, so as to improve the performance of the network via packet delivery rate and least bandwidth consumption. These behavior has affected the performance of query optimization during real-time applications. The range of listening capability of the nodes has not been properly prioritized while decoding the message via any routing path, which creates a higher chance for adversaries to inject false messages. Existing SLP protection algorithms have a significant impact on energy consumption. Deploying source aware is now critical to the success of wireless sensor network deployments. As of now, most of the users spends their time in social frames, the visibility given by IoT has to be ensured for better communication between objects.

In research activities, scalable services are obtained from different interconnected objects and thus, social relations with IoT systems has impressed the researchers. Most of the works focussed on relationships between human-object and object-objects and thus, the integration with IoT is a challenging tasks. In some cases, it scales down the performance of the system. So as to improve the usability and applicability of SioT, some nodes features are to be facilitated. Efficient discovery of the services will be achieved by social relationships between different objects. In some cases, establishing new services is a tedious task. Dynamic object selection inquires intelligent service features. Henceforth, objects has to be defined that can able to identify the new relationships from interconnected objects. Discovery of objects under SioT has become a critical issue in the aspects of large scale environment. Some cases has deployed agent based approaches, yet the challenges like scalability and interoperability have not been assured.

4. RESEARCH AIM & OUTCOMES

The prime objective of this work is to discover end-to-end secure routing protocols using hierarchical clustering approaches.

The following are the research objectives:

a) To find the lightweight solutions for challenges in IoT security.

b) To design a key agreement scheme via multicast communication model that assured all security parameters like confidentiality, integrity and availability.

c) To design a lightweight privacy preserving protocols for IoT environment.

d) To find a rapid and reliable security model that eliminates the processing overheads, bandwidth and energy consumption.

e) To ensure a source location privacy technique for social sensors in IoT domain.

5. RESEARCH METHODOLOGY

This section presents the proposed framework that covers the research objectives of the research study. The tentative steps will be as follows:

a) Create a network environment.

b) Initiates the number of sensor nodes i.e sink nodes, source nodes and destination nodes.

c) Initiating the security primitives of the networks.

d) Proposing a novel group key agreement protocols for IoT environment at three phases, namely,

- Deployment phase- Developing a key generation between gateway and proxy between entities.
- Key generation center- Computing the secret key among the entities.
- Session keys- Computing session keys, so as to assure the presence of authorized users.

e) Finding the scalability of the authentication models ie. How far its support the proposed system while member join/leave the groups.

d) Proposing a secured routing protocols for key agreement scheme.

e) Performing a hierarchical clustering approach for selecting the efficient cluster head, so as to achieve faster and reliable data communication purpose.

e) Proposing a formal security models among the entities in terms of key confidentiality, key integrity, freshness of key, secrecy maintenance in forward and backward models.

f) Along with that, mutual authentication between key agreement schemes and the social computing frameworks.

g) Proposing a detection framework for detecting reply attack resilience and impersonation attacks between the groups and its members.

6. EXISTING AND PROPOSED METHODOLOGY

6.1 Existing Methodology:

Existing source location privacy (SLP) protection methods primarily protect the SLP by expanding the number of routing paths available, such as phantom routing, multi-path routing, false information source injection, and other secure routing mechanisms. The existing SLP protection algorithms majorly protect the SLP by changing or enhancing the routing path, which greatly increases the energy overheads.

Table 1 Comparative analysis of Known System with Current System

SNO	KNOWN SYSTEM	CURRENT SYSTEM
1.	Source Location Privacy primarily protects the SLP by increasing the number of routing paths available.	Source Location Privacy primarily protects the SLP by reducing the number of routing paths available.
2.	Increasing the variety of routing paths, it increases the Energy Consumption.	Reduces the Energy Consumption.
3.	It does not have Key Generation for Encrypting the Data.	It is having Key Generation for Encrypting the Data.
4.	It does not have Hierarchical Clustering approach for secured information.	It is having Hierarchical Clustering approach for secured information.
5.	Performance evaluation will not be done for communication cost, Computation cost, Key Verification time, Key generation time and session time.	Performance evaluation will be done for communication cost, Computation cost, Key Verification time, Key generation time and session time.

6.2 Proposed Methodology:

To begin, propose and analyse a routing-based scheme based on a single intermediary node. Following that, two multi-intermediate node schemes are presented. We ran simulations on each of these schemes to assess their performance. The simulation results demonstrate that the proposed schemes perform very well in energy utilization, message delivery latency, and message delivery ratio. SIoT realization challenges by using the clustering approach to reach a destination with secured authentication and key generation in WSN. Where the protocols are classified based on single hop and multiple hop clustering approach and the energy distribution based on distance from source to destination with better clustering approach and increased node density. A large sensor network of SIoT applications, the ability to predict and secure the control system in peak time. Where saving a energy is also a part considering in the WSN and nodes may form clusters dynamically to reduce transmission distance to sink. First Initially, generate a network environment and initiate the nodes and primitives of the network. Then, a novel authenticated group key agreement for IoT environment will be created and develop a key generation using Advanced Multiple Encryption System (AMES). The proposed Advanced Multiple Encryption System is based on Message Queuing Telemetry Transport Protocol and Hardy Wall Algorithm. After that, Determine the scalability of the authentication models and propose a security routing protocol by using agglomerative hierarchical clustering approach. Performance evaluation will be done for communication cost, Computation cost , Key verification time , Key generation time and session time. Finally , compare the existing algorithms and proposed algorithms.

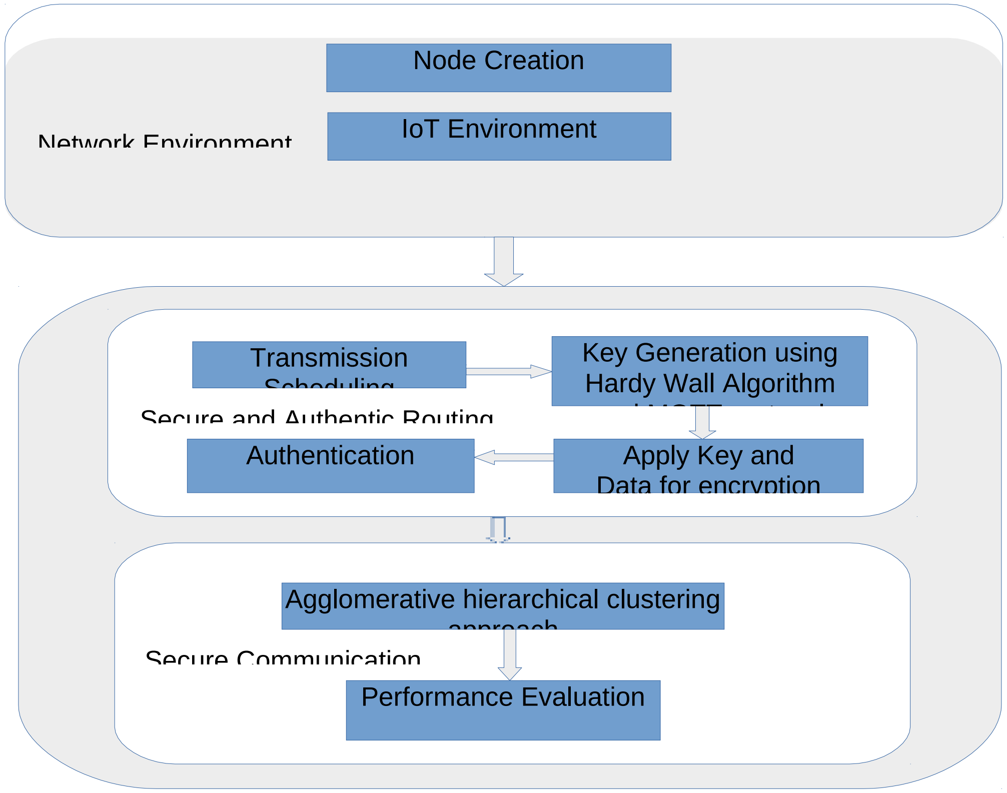
Node Creation
IoT Environment
Network Environment
Transmission Scheduling
Key Generation using Hardy Wall Algorithm
Secure and Authentic Routing
Authentication
Apply Key and Data for encryption
Agglomerative hierarchical clustering approach
Secure Communication
Performance Evaluation

Figure 2 System Architecture

6.3 Implementation Plan

Step 1:

Initially, generate a network environment and initiate the nodes and primitives of the network.

Step 2:

Then, a novel authenticated group key agreement for IoT environment will be created and develop a key generation using Advanced Multiple Encryption System (AMES). The proposed AMES system is based on Messaging Queuing Telemetry Transport (MQTT) Protocol and Hardy Wall Algorithm .

Step 3:

After that, Determine the scalability of the authentication models and propose a secured routing protocol by using agglomerative hierarchical clustering approach.

Step 4:

Performance evaluation will be done for communication cost, Computation cost, Key verification time, Key generation time and session time.

Step 5:

Finally, compare the existing algorithms and proposed algorithms.

7. MQTT (Message Queuing Telemetry Transport)

It stands for MQ Transport Telemetry. It is an extremely easy and lightweight (subscribe and publish) message protocol optimized for high latency, low bandwidth or unreliable networks for restricted devices and networks. Its key components are intended to decrease device requirements for network latency and resources while also ensuring supply prevention. Data is sent from a large number of devices to a single destination, the cloud, with Message Queuing Telemetry Transport, where the data can be processed, interpreted and forwarded.

A MQTT broker hosts the cloud, an intermediary between machines and other machines and/or individuals. MQTT Protocol act as an Agent/medium in between nodes. It acts as a request or response messages as it helps for exchange of data. Each source node has an unique Id using this Source node transformation of data is made. There would be a various sensors that would connected to the Broker nodes. The Broker node publish the data like node id, packet size, address of packet and time. There would be number of Source nodes, that would be connected to the broker node or MQTT. It would subscribe the data. Data Packets are sending through CBR (Constant Bit Rate) Packets. HTTP is a secure protocol that uses TCP/IP. Connection is accessible. However, connections have been made. Since the accessed data is encrypted, TCP is released for any access. HTTP transferred based on the connection between Internet Protocol address and Uniform Resource Locator is dynamically altered. In a nutshell, after several attempts, communication is established after the release of a link ended. MQTT reduces HTTP protocol overheads.

7.1 Comparative analysis of MQTT with HTTP Bandwidth

This section compares the bandwidth requirements of MQTT and HTTP. One is concerned with the properties of required bandwidth in relation to various devices and the number of topics. Another issue to consider is the required bandwidth's characteristics as a function of data volume variation. Figure 3 depicts these characteristics.

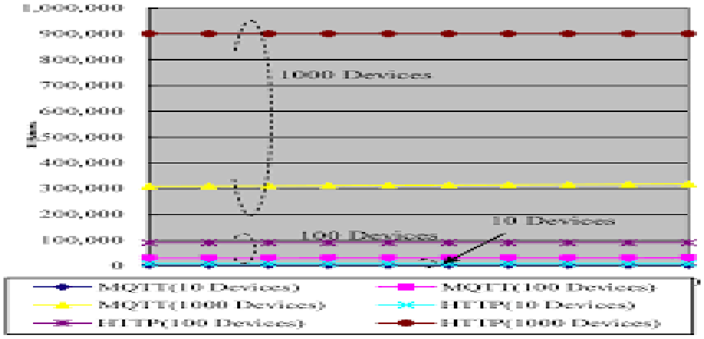

Figure 3 Overheads topic by MQTT[26]

In this Figure 3, the connection between MQTT topic total length and transmit bytes. Because the applications' payload size is zero in this case, the number of transmission bytes reflects only protocol overhead. Because HTTP lacks a topic definition, the number of bytes transmitted is determined by the horizon axis. A comparison of HTTP and MQTT performance has been made. MQTT mitigates and it performs better than HTTP.

8. Hardy Wall Algorithm

The Hardy Wall Encryption Algorithm is designed using Fermat's Theorem. Algorithms based on Fermat's theorem are the most common for factorization. The advanced method of factorizing multi-bit numbers is well explained by using Fermat's Theorem.

$$\mathbf{HW = ((a \bmod b) / RN) + W + S \quad (1)}$$

where: HW – Hardy Wall Algorithm
a – Alice Value
b – Bob Value

RN – Random Number
W – No. of Words
S – Sequence Number

By using this Hardy Wall Algorithm, the Energy Consumption gets decreased. One of the most critical criteria for a network is transmission speed. Regardless of how reliable the network is, if the transmission speed is slow, the entire network will fail to function in real time. Networks must be able to communicate with one another quickly by exchanging messages, and without this, an effective infrastructure cannot be built.

8.1 Hardy Wall Algorithm

```
Input: List of Words
 W and Sequence Number
 S Create a Hardy Wall HW to W and S
for each Words W and Sequence, Number S do
Generate Alice value a, Bob Value b and
 Random Number RN
 Modulus a with b (a mod b) namely key K
Divide K with RN (K/RN)
Add (K/RN) with W and S
end for
If W and P is Encrypted E(W, S)
Save E(W, S)
Initialize the communication with E(W, S)
else
Stop the initialization
 end if
Output the best Encrypted formula
```

The Evaluation of the Hardy Wall Algorithm has observed to be greater than the Fermat's theorem.

9. Conclusion

Social Internet of Things (SIoT) is considered to be the tentative performance metrics, Object Discovery, Complexity and very huge risk factors are interest. Source location privacy plays a vital role for Wireless Sensor Networks. Simulations can be carried out and test the result for each of these patterns. Cost metrics is one of the important metrics which is least focussed by many researchers. Therefore, Cost analysis in order of computational, storage and communication overheads. Computation cost: Different hash functions will be employed, so as to design a lightweight key generation schemes. Communication cost of this work is to lower the communication cost and thus, it will be focussed for resource constrained nodes. By using this MQTT and Hardy wall algorithm schemes can achieve excellent results in terms of energy consumption, message delivery ratio and message delivery latency. Length of the message sent and received will be computed. Storage cost will be computed on the basis of bytes stored by a node. Key generation time, Key verification time and Session key time and its cost were calculated.

References

1 Ammar, Mahmoud, Giovanni Russello and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks”. Journal of Information Security and Applications38 (2018): 8-27.

2 Jayakumar, Hrishikesh, et al. "Powering the Internet of Things". Proceedings of the 2014 International symposium on Low power electronics and design. ACM, 2014.

3 Lin Jie, et al. "A survey on Internet of Things: Architecture, Enabling technologies, security and privacy, and applications" . IEEE Internet of Things Journal 4.5 (2017): 1125-1142.

4 AlFuqaha , Ala, et al. "Internet of Things: A Survey on enabling technologies, protocols, and applications." IEEE Communications Surveys & Tutorials 17.4 (2015): 2347-2376.

5 Agrawal, Shashank, and Dario Vieira, "A survey on Internet of Things." Abakós 1.2 (2013): 78-95.

6 Veltri, Luca, et al. "A novel batch-based Group Key Management Protocol applied to the Internet of Things." Ad Hoc Networks 11.8 (2013): 2724-2737

7 Abdmeziem, Mohammed Riyadh, Djamel Tandjaoui, and Imed Romdhani. "A Decentralized batch-based Group key Management Protocol for mobile Internet of Things (IoT)". Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on. IEEE, 2015.

8 Li, Yue. "Design of a Key Establishment Protocol for Smart Home Energy Management System." Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on. IEEE, 2013.

9 Hendaoui, Fatma, Hamdi Eltaief, and Habib Youssef. "A Collaborative Key Management Scheme for Distributed Smart Objects". Transactions on Emerging Telecommunications Technologies 29.6 (2018): e3198.

10 Matsumoto, Ryutaroh. "Strong Security of the Strongly Multiplicative ramp secret sharing based on algebraic curves". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 98.7 (2015): 1576-1578.

11 Bamasag, Omaimah, and Kamal Youcef Toumi. " Efficient multicast authentication in Internet of Things".Information and Communication Technology Convergence (ICTC), 2016 International Conference IEEE, 2016.

12 Dahshan, Hisham. "An Elliptic Curve Key Management scheme for Internet of Things". International Journal of Applied Engineering Research ,11.20 (2016): 10241- 10246.

13 Porambage, Pawani, et al. "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications". IEEE Access 3.1 (2015): 1503-1511.

14 Das, Ashok Kumar, et al. "A Dynamic password-based user authentication scheme for hierarchical wireless sensor networks". Journal of Network and Computer Applications35.5 (2012): 1646-1656.

15 Turkanović, Muhamed, Boštjan Brumen, and Marko Hölbl. "A novel user authentication and Key agreement scheme for heterogeneous ad hoc Wireless Sensor Networks, based on the Internet of Things notion". Ad Hoc Networks 20 (2014): 96-112.

16 He, Debiao, Neeraj Kumar, and Naveen Chilamkurti. "A Secure temporal-credential based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks". Information Sciences 321 (2015): 263-277

17 Ozturk, Celal, Yanyong Zhang, and Wade Trappe. "Source location privacy in Energy-constrained Sensor network routing". Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM, 2004.

18 Jhumka, Arshad, Matthew Leeke, and Sambid Shrestha. "On the use of fake sources for source location privacy: Trade-offs between energy and privacy". The Computer Journal 54.6 (2011): 860-874.

19 Rodrigo Roman et al, "Key management systems for sensor networks in the context of the Internet of Things", Computers & Electrical Engineering • March 2011, DOI: 10.1016/j.compeleceng.2011.01.009

20 Garcia-Morchon, Oscar, et al. "DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs)". (2013).

21 J. Long, A. Liu, "An Energy-efficient and sink-location Privacy enhanced scheme for WSNs through Ring based routing," Journal of Parallel & Distributed Computing , 2015, pp: 47-65.

22 A. Liu, D. Zhang, P. Zhang, G. Cui, and Z. Chen, "On mitigating hotspots to maximize network lifetime in multi-hop wireless sensor network with guaranteed transport delay and reliability," Software: Practice and Experience, 2014, Vol. 7, No. 3, pp: 255-273.

23 B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Towards a statistical framework for source anonymity in sensor networks," IEEE Transactions on Mobile Computing, 2013, Vol. 12, No. 2, pp: 248-260.

24 P. Kumar, JP. Singh, P. Vishnoi, and MP. Singh, "Source location privacy using multiple- phantom nodes in WSN," TENCON, 2015, pp: 1-6.

25 T. Qiu, AY. Zhao, RX. Ma, V. Chang, FB. Liu, ZJ. Fu. "A Task-Efficient Sink Node Based on Embedded Multi-core SoC for Internet of Things," Future Generation Computer Systems, 2017.

26 Yokotani, T., & Sasaki, Y. (2016). Comparison with HTTP and MQTT on required network resources for IoT. 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC). doi:10.1109/iccerec.2016.7814989